



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1400
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/775,205

02/01/2001

Alan Boate

RIDM.P-002

7111

32692

7590

08/09/2006

3M INNOVATIVE PROPERTIES COMPANY

PO BOX 33427

ST. PAUL, MN 55133-3427

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 08/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/775,205

Applicant(s)

BOATE ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) 22 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 May 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's **amendments and arguments** filed on 05/18/2006 with respect to **amended** claims 1, 9, and 17, have been considered but are moot in view of the new ground(s) of rejection.
2. Examiner accepts the amended drawings and abstract in view of the Examiner's objection.
3. Claims 1-21 are presented for examination.
4. Claim 22 has been canceled.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 8-9, 13, 16-19, and 21 have been fully considered but they are not persuasive.

The appellant's first argument concerns Scott, Davis and Addy failure to disclose "wherein, during a currently logged-in session of the user associated with the personal digital identifier device, a policy manager component directs at least one of the workstations to blank out a respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the currently logged-in session (remarks page 12 lines 10-page 14 lines 22)" as amended and recited in claims 1, 9 and 17, the Examiner changes the ground of rejection (see, claims 1, 9, and 17 rejection in current

office action or the well-known proximity authorization of wireless devices Domb et al. US 6,594,762 B1).

As per appellant's concerning Scott, Davis and Addy failure to describe "a personal digital identifier device having a processor operable for generation said private key held by said personal digital identifier device and outputting said generated public key for transmission by said transceiver (*remarks page 14 lines 23-page 15 lines 3*)" as recited in claims 1, 9, and 17. Scott stores private key in the PDI 6 held by PDI 6 and outputs public key for transmission by said transceiver to the host facility 4 (see, col. 10 lines 50-55). Even though Scott does not explicitly teach the private and corresponding public keys are generated inside the PDI 6 device or generated outside and transmitted to the PDI 6 device, Appellant's argument regarding wireless device or PDI generating private public key pairs is very well known at the time of the invention (see, claims 1, 9, and 17 of current rejection or Labaton US PG PUBs 2002/0191765 at claim 5).

As per appellant's concerning Scott, Davis and Addy failure to describe "generating a master template for a biometric on the portable device itself without requiring the master biometric template be transmitted to the device (*remarks page 15 lines 3-6*)" as recited in claims 1 and 9. The examiner respectfully disagrees with the appellant's contentions and would like to refer to col. 6 lines 56-61, col. 3 lines 42-62, and col. 4 lines 13-43 wherein Scott discloses generating master template for fingerprint/biometrics and storing master templates on the PDI 6, and comparing fingerprints image of a user's fingerprint being placed on a platen of a portable user device with the master template stored on PID 6 and if verified/authentic generating an access signal with the user device and transmitting the access signal to allow access to the secure

facilities/host. The access signal including only an ID code associated only with the user device, button press information representing a requested function, and a synchronization counter associated with the user device. PDI 6 does not transmit the PDI 6 generated biometric template to host but access signal. **Moreover**, the Office provided the Bolle reference for well-known and argued subject matter generating biometric master template locally in a wireless device and never transmitting the biometric master template from the wireless device (see, Office action mailed on 08/11/2005 page 8 lines 9-13) because it would prevent an intruder from accessing master template biometric data by storing it locally and never transmitting it from the wireless device (see, Bolle USPN 6,819,219 col. 7 lines 63-65). And this limitation cannot be argued for claim 17 because it is not claimed for claim 17.

As per appellant's concerning Scott failure to disclose a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device, said device holder comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder (*remark page 15 lines 8-14*)" as recited in claims 8. The examiner respectfully disagrees with the appellant's contentions and would like to refer to fig. 5B element 58 (device holder), fig. 4A element 44 (housing), and col. 6 lines 29-53, wherein Scott discloses a belt clip for the PID 6. The device holder holds the PID 6 and communications connectors of the PID 6 are certainly communicated to the host facility 30 and access is provided based on authentication.

(Appellant is provided a second reference, Davis et al. USPN 6,088,450 fig. 1 element 140, for reference, see current rejection claim 8).

As per appellants concerning Scott failure to disclose "... base units receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelop (*remark page 15 lines 15-page 16 line 4*)" as recited in claim 19. The Examiner disagrees with the Appellant's contention. Scott discloses plurality customers having PDI 6 wireless device to get access to host facilities/banks and the wireless polling signal is exchanged within the rang to provide access to plurality of ATMs connected to a plurality of banks, and the PDI 6 wireless device is identified and located in the rang, wherein is the ATM is the base unit and the bank office is the workstation. (See, col. 10, lines 58-65 of Scott, col. 6, lines 29-40 and col. 11, lines 46-59). Moreover the argued subject matter cannot be argued for claim 13 because it is not claimed in claim 13. Appellant is provided a reference to refer the well-known exchanging polling signal to determine if the attachable and detachable wireless device holder is within the base unit associated area (see, Rebstock et al. col. 5 lines 8-13, abstract and col. 3 lines 3-54 and fig. 1 or the claim 19 of the current office action).

As per Appellant's concerning Scott failure to disclose "the envelop has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation, (*remark page 16 lines 5-16*)" as recited on claims 16 and 18. The Examiner disagrees with the Appellant's contention. Scott discloses a range that has a shape and area (see, col. 10 lines 58-67,

and col. 9 lines 29-36). Moreover Doub et al. teaches the shape and area, location proximity and observer as claimed in claims 16 and 18 (see, col. 3 lines 19-43).

As per Appellant's concerning Scott failure to disclose "... each of said registrar, guarantor and user remain within said envelope during said registering of said user (*remark page 16 lines 24-page 17 lines 3*), as recited in claim 21" The examiner disagree with Appellant and would like to refer to Scott col. 3 lines 20-63, col. 11, lines 46-59, and fig. 1 wherein Scott discloses the trusted third party 39, host system 30 and PID 6 in the same envelop and performing registration.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott et al. (Scott, U.S. Patent No. 6,484,260) in view of Davis (U.S. Patent No. 5,568,552), Labaton US PG PUBs 2002/0191765 A1, and Doub et al. USPN 6,594,762 B1.

Regarding claims 1, 9, and 17, Scott et al. teaches a method/security system for controlling access to a computer network at a network access point comprising a workstation, said system comprising:

- a personal digital identifier device (fig. 1, ref. num 6) comprising:
 - a wireless communications component comprising a transceiver (fig. 1, ref. num 26 and 28 and col. 6, lines 52-53),
 - a biometric acquisition component for obtaining a user's input biometric and producing a digital representation thereof (fig. 1, ref. num 11, 12, 14, and 15 and col. 6, lines 41-47),
 - a processor configured for communicating with said transceiver and said biometric component (fig. 1, ref. num 16, 18, 20, 22, and 23) and operable for:
 - evaluating whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component and generating a matching signal when such a correspondence is determined (col. 10, lines 15-29),
 - a private key to be held by said personal digital identifier device and a public key corresponding thereto and outputting said generated public key for transmission by said transceiver (col. 10, lines 50-55),
 - secure storage containing said master template of a user's biometric, said generated private key (fig. 1, ref. num 20 and col. 8, lines 34-36),
 - said personal digital identifier device being configured for producing, using said generated private key, a challenge response message following said generating of said matching signal in response to a challenge received from said security manager component and for transmitting said response message (col. 2, lines 28-39), and

said personal digital identifier device being configured to prevent transmission of any of said master template of a user's biometric and said private key (col. 11, lines 56-59),

- a base unit associated with said workstation and configured for initiating and maintaining wireless communications with said personal digital identifier device (fig. 1, ref. num 4, 8, 38, and 40),

said communications extending over an area defined by an envelope associated with said workstation (col. 10, lines 58-63), and,

- a central server having access to network storage and utilizing said security manager component and said personal digital identifier device for authenticating said user (fig. 1, ref. num 32, 34, and 36),

said network storage containing a public key corresponding to said private key generated by said personal digital identifier device (col. 7, lines 2431).

Scott does not teach a processor used for: producing a digital signature using said private key and, verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; the secure storage containing said public key for said private key associated with said security manager component; and the challenge response message is digitally signed.

Davis teaches:

- a processor used for:
producing a digital signature using said private key (col. 5, lines 27-30) and,

verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component (col. 4, lines 54-65);

- the secure storage containing said public key for said private key associated with said security manager component (col. 4, lines 40-53); and
- the challenge response message is digitally signed (col. 4, lines 3-10).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a processor used for: producing a digital signature using said private key and, verifying that an encrypted received message is from a security manager component using a public key for a private key associated with said security manager component; the secure storage containing said public key for said private key associated with said security manager component; and the challenge response message is digitally signed, as taught by Davis, with the method/system of Scott.

It would have been obvious to combine the steps taught by Davis, with the method/system of Scott because the digital signature and digitally signed response message provide non-repudiation from the PDI to the base unit; this enables the base unit to trust that the PDI in question is the PDI that is supposed to be used. Storing the public key of the security manager in the secure storage area of the PDI, which corresponds to the private key stored in the security manager, to verify encrypted received messages enables the PDI to verify the base units identity. Any encrypted message sent from the security manager to the PDI can be checked for non-repudiation by using the corresponding public key that is stored in the PDI.

Scott and Davis fail to explicitly teach the private/public pair keys used in the PDI 6 wireless device are generated inside the PDI 6 device.

However Labaton discloses the well-known and argued subject matter generating private key and the corresponding public key in the wireless device (see claim 5).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Labaton within the combination system of Scott and David because it would be secure to generate it inside the wireless PDI device. One would be motivated to do so because the private key would not be known by any other device even the generator of the external device and secure the process.

Scott, Davis, and Labaton teach all the subject matter as described above. **Scott discloses a user of PDI approaching an ATM/base unit. Once the user is within a certain distance, the exchanging of ID codes and authenticating of the PDI user occurs. Only after a successful authentication will the user be able to see information displayed of the ATM. No information is displayed for non-authorized/not registered PDI user.**

However Scott, Davis, and Labaton fail to explicitly disclose wherein, during a current logged-in session of the user associated with the personal digital identifier device, a policy manager component directs at least one of the workstations to blank out respective screen when a second personal digital identifier device is detected at a location within an envelope until such time as a user registered to said second personal digital identifier device is biometrically identified to have permission to view data of the current logged-in session, as amended.

Doub et al. discloses a method of wireless authorized remote device 110 (*PDI*) authentication in a range (*envelope*) distance proximity (col. 1 lines 39-col. 2 lines 47) and a method of denying a display access of personal data/sensitive data to unauthorized remote device (*second personal PDI*) while the authorized remote device is in logged-in session and away from

the computer, unless the unauthorized remote device is a registered/known device and the authentication code generated at registration match (see, col. 1 lines 12-35, fig. 1, and col. 4 lines 26-45).

It would have been obvious to one ordinary skill in the art at the time of the invention was made to employ and modify the teachings of Doub et al. within the combination system because it would protect the display of sensitive data to unauthorized user. One would have been motivated to do so because it would protect the authorized user's sensitive data from being rendered by unauthorized user until the authentication code of the unauthorized remote device match with registered authentication code (see, col. 1 lines 12-35, and col. 4 lines 26-45).

Regarding claims 2 and 10, Scott further teaches wherein said biometric component includes a transducer (see col. 1, lines 66-67 of Scott).

Regarding claims 3 and 12, Scott further teaches wherein said base unit regularly transmits a first signal to said personal digital identifier device and said personal digital identifier device automatically transmits a response signal in response thereto when said personal digital identifier device is within said envelope (see col. 10, lines 58-65 of Scott).

Regarding claims 4 and 14, Scott further teaches wherein all data held in said secure storage is by itself non-identifiable of said user (see col. 8, lines 34-38 of Scott).

Regarding claim 5, Scott further teaches wherein said transducer comprises a solid-state fingerprint sensor (see col. 6, lines 54-66 of Scott).

Regarding claim 6, Scott further teaches wherein said transceiver transmits and receives optical signals (see col. 7, lines 35-50 of Scott).

Regarding claim 7, Scott further teaches wherein said transceiver transmits and receives radio frequency signals (see col. 7, lines 35-50 of Scott).

Regarding claim 8, Scott et al. and Davis teach in combination with a device holder wherein said device holder is configured to co-operate with said housing of said personal digital identifier device such that said personal digital identifier device is held by said holder device when it is appropriately positioned relative to said holder device comprising a communications connector for communicatively coupling said personal digital identifier device directly to one said workstation when said personal digital identifier device is held by said device holder (see fig. 5B, ref. num 58, fig. 1 element 140 fig. 4A element 44 (housing), and col. 6 lines 29-53).

Appellant is provided Davis et al. USPN 6,088,450, for further reference that the device holder belt clip has communications connector to communicate the PDI with the host device (see, Davis et al. fig. 1 element 120, 140, and 110, and col. 3 lines 52-67).

Regarding claim 11, Scott further teaches wherein said workstation is a personal computer (see col. 6, lines 31-34 of Scott).

Regarding claim 13, Scott further teaches a system comprising a plurality of said personal digital identifier devices, a plurality of workstations and a plurality of base units wherein a base unit is associated with each said workstation (see col. 6, lines 29-40 and col. 11, lines 46-59 of Scott,

each customer has a PDI, each ATM is connected to a bank office, wherein the ATM is the base unit and the bank office is the workstation), each said base unit transmitting a polling signal to each said personal digital identifier device within said base unit's associated envelope following said base unit's receipt of said response signal from each said personal digital identifier device (see col. 10, lines 58-65 of Scott).

Regarding claims 15 and 20, Scott further teaches wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope (see col. 10, line 58 through col. 11, line 33 of Scott).

Regarding claims 16 and 18, Scott et al. and Doub et al. teach wherein said envelope has a shape and area which are configured to encompass those locations proximate to said workstation at which an observer may read and/or understand information displayed on a screen of said workstation (see, Scott col. 9, lines 29-38 and col. 10, lines 58-63 of Scott, and Doub et al. col. 3 lines 19-43).

Regarding claim 19, Scott et al. further discloses a method and further comprising, following said base unit's receipt of said response signal from said personal digital identifier device, transmitting from said base unit a polling signal to said personal digital identifier device for determining whether said personal digital identifier device remains located within said base unit's associated envelope (See, col. 10, lines 58-65 of Scott, col. 6, lines 29-40 and col. 11, lines 46-59). (For the sake of the Appellant's argument, regarding this claim the Examiner provided a

second reference that discloses transmitting and sending polling signals between wireless devices and base units to determine the wireless device of the patient/user location within the rang/envelop see abstract and col. 3 lines 3-54. One would have been motivated to determine the location of the wireless device because it would provide information to the host device based on location of the wireless device, in the range.

Regarding claim 21, Scott further teaches further comprising initially registering said user by a registrar in the presence of a guarantor, said registrar and guarantor each being a registered user of the computer network and said registrar having access to the computer network and verified by said security manager component to have registration privileges, and requiring that said guarantor provide to said security manager component a biometrically digitally signed message to authenticate said guarantor and that each of said registrar, guarantor and user remain within said envelope during said registering of said user (see col. 11, lines 46-59 and fig. 1 of Scott).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

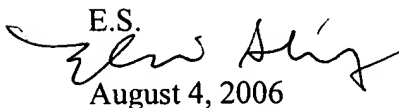
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

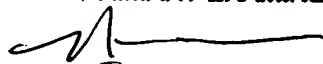
will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

August 4, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

8/7/06